Long zero-free sequences in finite cyclic groups

Svetoslav Savchev [1], Fang Chen [a]

[a] *Oxford College of Emory University, Oxford, GA 30054, USA*

Abstract

A sequence in an additively written abelian group is called zero-free if each of its nonempty subsequences has sum different from the zero element of the group. The article determines the structure of the zero-free sequences with lengths greater than $n/2$ in the additive group $\mathbb{Z}_n$ of integers modulo n. The main result states that for each zero-free sequence $(a_i)_{i=1}^{\ell}$ of length $\ell > n/2$ in $\mathbb{Z}_n$ there is an integer g coprime to n such that if $\overline{ga_i}$ denotes the least positive integer in the congruence class ga_i (modulo n), then $\Sigma_{i=1}^{\ell}\overline{ga_i} < n$. The answers to a number of frequently asked zero-sum questions for cyclic groups follow as immediate consequences. Among other applications, best possible lower bounds are established for the maximum multiplicity of a term in a zero-free sequence with length greater than $n/2$, as well as for the maximum multiplicity of a generator. The approach is combinatorial and does not appeal to previously known nontrivial facts.

Key words: zero-sum problems, zero-free sequences

1 Introduction

Among n arbitrary integers one can choose several whose sum is divisible by n. In other words, each sequence of length n in the cyclic group of order n has a nonempty subsequence with sum zero. This article describes all sequences of length greater than $n/2$ in the same group that fail the above property.

Here and henceforth, n is a fixed integer greater than 1, and the cyclic group of order n is identified with the additive group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ of integers modulo n. A sequence in $\mathbb{Z}_n$ is called a *zero sequence* or a *zero sum* if the sum of its terms is the zero element of $\mathbb{Z}_n$. A sequence is *zero-free* if it does not contain nonempty zero subsequences.

We study the general structure of the zero-free sequences in $\mathbb{Z}_n$ whose lengths are between $n/2$ and n. Few nontrivial related results are known to us,

[1] No current affiliation.

of which we mention only one. A work of Gao [6] characterizes the zero-free sequences of length roughly greater than $2n/3$. On the other hand, structural information about shorter zero-free sequences naturally translates into knowledge about problems of significant interest. Several examples to this effect are included below. The main result provides complete answers to a number of repeatedly explored zero-sum questions.

Our objects of study can be characterized in very simple terms. To be more specific, let us recall several standard notions.

If g is an integer coprime to n, multiplication by g preserves the zero sums in $\mathbb{Z}_n$ and does not introduce new ones. Hence a sequence $\alpha = (a_1, \ldots, a_k)$ is zero-free if and only if the sequence $g\alpha = (ga_1, \ldots, ga_k)$ is zero-free, which motivates the following definition.

For sequences α and β in $\mathbb{Z}_n$, we say that α is *equivalent* to β and write $\alpha \cong \beta$ if β can be obtained from α through multiplication by an integer coprime to n and rearrangement of terms. Clearly $\cong$ is an equivalence relation.

If $\alpha = (a_1, \ldots, a_k)$ is a sequence in $\mathbb{Z}_n$, let $\overline{a_i}$ be the unique integer in the set $\{1, 2, \ldots, n\}$ which belongs to the congruence class a_i modulo n, $i = 1, \ldots, k$. The number $\overline{a_i}$ is called the *least positive representative* of a_i. Consequently, the sum $L(\alpha) = \sum_{i=1}^{k} \overline{a_i}$ will be called the *sum of the least positive representatives* of α.

Now the key result in the article, Theorem 8, can be stated as follows:

Each zero-free sequence of length greater than $n/2$ in $\mathbb{Z}_n$ is equivalent to a sequence whose sum of the least positive representatives is less than n.

This statement reduces certain zero-sum problems in cyclic groups to the study of easy-to-describe positive integer sequences. Thus all proofs in Sections 5–8 are merely short elementary exercises.

The approach of the article is combinatorial and does not follow a line of thought known to us from previous work. The exposition is self-contained in the sense that it does not rely on any nontrivial general fact. Sections 2 and 3 are preparatory. The main result is proven in Section 4.

For a sequence α in $\mathbb{Z}_n$, the number $Index(\alpha)$ is defined as the minimum of $L(g\alpha)$ over all g coprime to n. Section 5 contains the answer, for all n, to the question about the minimum $\ell(\mathbb{Z}_n)$ such that each minimal zero sequence of length at least $\ell(\mathbb{Z}_n)$ in $\mathbb{Z}_n$ has index n.

Issues of considerable interest among the zero-sum problems are the maximum multiplicity of a term in a zero-free sequence, and of a generator in particular. Sections 6 and 7 provide exhaustive answers for zero-free sequences of all lengths $\ell > n/2$ in $\mathbb{Z}_n$. Best possible lower bounds are established in both cases, which improves on earlier work of Bovey, Erdős and Niven [2], Gao and Geroldinger [7], Geroldinger and Hamidoune [8].

In Section 8 we introduce a function closely related to the zero-free sequences in cyclic groups. This is an analogue of a function defined by Bialostocki and Lotspeich [1] in relation to the theorem of Erdős, Ginzburg and Ziv [5]. Theorem 8 enables us to determine the values of the newly defined function

in a certain range. An explicit description of the zero-free sequences with a given length $\ell > n/2$ in $\mathbb{Z}_n$ is included in Section 9.

2 Preliminaries

Several elementary facts about sequences in general abelian groups are considered below. We precede them by remarks on terminology and notation. The *sumset* of a sequence in an abelian group G is the set of all $g \in G$ representable as a nonempty subsequence sum. The cyclic subgroup of G generated by an element $g \in G$ is denoted by $\langle g \rangle$; the order of g in G is denoted by ord(g).

Proposition 1 *For a zero-free sequence $(a_1, \ldots, a_k)$ in an abelian group, let Σ_i be the sumset of the subsequence $(a_1, \ldots, a_i)$, $i = 1, \ldots, k$. Then Σ_{i-1} is a proper subset of Σ_i for each $i = 2, \ldots, k$. Moreover, the subsequence sum $a_1 + \cdots + a_i$ belongs to Σ_i but not to Σ_{i-1}. In particular, $a_1 + \cdots + a_k$ belongs to Σ_k but not to any Σ_i with $i < k$.*

PROOF. Since $\Sigma_{i-1} \subseteq \Sigma_i$ and $a_1 + \cdots + a_i \in \Sigma_i$, it suffices to prove that $a_1 + \cdots + a_i \notin \Sigma_{i-1}$, $i = 2, \ldots, k$. Suppose that $a_1 + \cdots + a_i \in \Sigma_{i-1}$ for some $i = 2, \ldots, k$. Then $a_1 + \cdots + a_i = \sum_{j \in J} a_j$ for a nonempty subset J of $\{1, \ldots, i-1\}$. Each term on the right-hand side is present on the left-hand side, and a_i is to be found only on the left. So canceling yields a nonempty zero sum in $(a_1, \ldots, a_k)$, which contradicts the assumption that it is zero-free. $\square$

Proposition 1 states that, for a zero-free sequence $\alpha = (a_1, \ldots, a_k)$, the sumset of the subsequence $(a_1, \ldots, a_{i-1})$ strictly increases upon appending the next term a_i, $i = 2, \ldots, k$. If the increase of the sumset size is exactly 1, we say that a_i is a 1-*term* for α. Naturally, the property of being a 1-term is not necessarily preserved upon rearrangement of terms.

The next statement contains observations on 1-terms. Parts a) and b) seem to be folklore and can be found for instance in [10].

Proposition 2 *Let $\alpha = (a_1, \ldots, a_k)$ be a nonempty zero-free sequence with sumset Σ in an abelian group G. Suppose that, for some $b \in G$, the extended sequence $\alpha \cup \{b\} = (a_1, \ldots, a_k, b)$ is zero-free and b is a 1-term for $\alpha \cup \{b\}$. Then:*

- *a) Σ is the union of a progression $\{b, 2b, \ldots, sb\}$, where $1 \le s < \mathrm{ord}(b)-1$, and several (possibly none) complete proper cosets of the cyclic subgroup generated by b;*
- *b) the sum of α equals sb;*
- *c) b is the unique element of G that can be appended to α as a last term so that the resulting sequence is zero-free and ends in a 1-term.*

PROOF. Parts a) and b) are proven in [10]. For part c), let $c \in G$ be such that the sequence $\alpha \cup \{c\} = (a_1, \ldots, a_k, c)$ is zero-free and c is a 1-term for $\alpha \cup \{c\}$. We prove that $c = b$. Because b is a 1-term for $\alpha \cup \{b\}$, in view of a) we have

$\Sigma = \{b, 2b, \ldots, sb\} \cup C_1 \cup \cdots \cup C_m$, where $1 \le s < \mathrm{ord}(b)-1$ and $C_1, \ldots, C_m$ are complete proper cosets of the subgroup $\langle b \rangle$ generated by b. The sumset Σ' of $\alpha \cup \{c\}$ contains the progression $P = \{c, c+b, \ldots, c+sb\}$ whose length $s+1$ is at least 2. Since c is a 1-term for $\alpha \cup \{c\}$, it follows that P intersects $\{b, 2b, \ldots, sb\}$ or one of $C_1, \ldots, C_m$. By b), P contains the sum $c+sb$ of $\alpha \cup \{c\}$, which is an element of $\Sigma' \setminus \Sigma$ in view of Proposition 1. Hence $P \cap C_i = \emptyset$ for all $i = 1, \ldots, m$, or else $c + sb \in \Sigma$. Thus P intersects $\{b, 2b, \ldots, sb\}$, and $0 \notin P$ implies $c = xb$ for some integer x satisfying $1 \le x \le s$. Hence the progression $\{b, 2b, \ldots, (s+x)b\}$ is contained in Σ'. Now we see that the size of Σ grows exactly by 1 upon appending c only if $x = 1$, i. e. $c = b$. $\square$

A zero-free sequence in a finite abelian group G is *maximal* if it is not a subsequence of a longer zero-free sequence in G. Let α be a zero-free sequence in G whose sumset does not contain at least one nonzero element g of G. Then $\alpha \cup \{-g\}$ is a longer zero-free sequence containing α. This remark and Proposition 1 show that a zero-free sequence in G is maximal if and only if its sumset is $G \setminus \{0\}$. The same remark (with Proposition 1 again) yields a quick justification of the next statement. We omit the proof.

Proposition 3 *Each zero-free sequence in a finite abelian group can be extended to a maximal zero-free sequence.*

3 Behaving sequences

A positive integer sequence with sum S will be called *behaving* if its sumset is $\{1, 2, \ldots, S\}$. The ordering of the sequence terms is not reflected in the definition. However, assuming them in nondecreasing order enables one to state a convenient equivalent description. Its sufficiency part is a problem from the 1960 edition of the celebrated Kürschák contest in Hungary, the oldest mathematics competition for high-school students in the world.

Proposition 4 *A sequence $(s_1, \ldots, s_k)$ with positive integer terms in nondecreasing order $s_1 \le \cdots \le s_k$ is behaving if and only if*

$$s_1 = 1 \qquad \textit{and} \qquad s_{i+1} \le 1 + s_1 + \cdots + s_i \quad \textit{for all } i = 1, \ldots, k-1.$$

PROOF. Denote $S = s_1 + \cdots + s_k$ and suppose that the sequence is behaving; then its sumset is $\Sigma = \{1, 2, \ldots, S\}$. Since $1 \in \Sigma$ and $s_i \ge 1$ for all i, it follows that $s_1 = 1$. For each $i = 1, \ldots, k-1$, let $T_i = 1 + s_1 + \cdots + s_i$. Clearly $T_i \le S$, hence $T_i \in \Sigma$. Also $T_i > s_1 + \cdots + s_i$, so the subsequence whose sum equals T_i contains a summand s_j with index j greater than i. Therefore $T_i \ge s_j \ge s_{i+1}$, as desired.

Conversely, let $s_1 = 1$ and $s_{i+1} \le 1 + s_1 + \cdots + s_i$, $i = 1, \ldots, k-1$. Denoting $S_k = s_1 + \cdots + s_k$, we prove by induction on k that the sumset of $(s_1, \ldots, s_k)$ is $\{1, 2, \ldots, S_k\}$. The base $k = 1$ is clear. For the inductive step, let Σ_{k-1} and Σ_k be the sumsets of $(s_1, \ldots, s_{k-1})$ and $(s_1, \ldots, s_{k-1}, s_k)$, respectively.

Since $\Sigma_{k-1} = \{1, 2, \ldots, S_{k-1}\}$ by the induction hypothesis, it follows that $\Sigma_k = \{1, 2, \ldots, S_{k-1}\} \cup \{s_k, s_k + 1, \ldots, s_k + S_{k-1}\}$. In view of the condition $s_k \leq 1 + S_{k-1}$, we obtain $\Sigma_k = \{1, 2, \ldots, s_k + S_{k-1}\} = \{1, 2, \ldots, S_k\}$. The induction is complete. $\square$

A simple consequence of Proposition 4 proves essential for the main proof.

Proposition 5 *Let k be a positive integer. Each sequence with positive integer terms of length at least $k/2$ and sum less than k is behaving.*

PROOF. Denoting the sequence by $(s_1, \ldots, s_\ell)$ and assuming $s_1 \leq \cdots \leq s_\ell$, we check the sufficient condition of Proposition 4. Given that $\ell \geq k/2$ and $\Sigma_{i=1}^{\ell} s_i < k$, it is easy to see that $s_1 = 1$. Suppose that $s_{i+1} \geq 2 + s_1 + \cdots + s_i$ for some $i = 1, \ldots, \ell - 1$. Then $s_j \geq i + 2$ for all $j = i + 1, \ldots, \ell$. Therefore

$$k > \Sigma_{i=1}^{\ell} s_i \geq i + (\ell - i)(i + 2) = 2\ell + i(\ell - i - 1) \geq k + i(\ell - i - 1) \geq k,$$

which is a contradiction. The claim follows. $\square$

Now we introduce a key notion. Let G be an abelian group and g a nonzero element of G. A sequence α in G will be called *behaving with respect to g* or *g-behaving* if it has the form $\alpha = (s_1 g, \ldots, s_k g)$, where $(s_1, \ldots, s_k)$ is a behaving positive integer sequence with sum $S = s_1 + \cdots + s_k$ less than the order of g in G.

It follows from the definition that $1 \leq s_i < \operatorname{ord}(g)$ for $i = 1, \ldots, k$. All terms of α are contained in the cyclic subgroup $\langle g \rangle$ generated by g. Moreover, since the sumset of $(s_1, \ldots, s_k)$ is $\{1, 2, \ldots, S\}$, the sumset of α is the progression $\{g, 2g, \ldots, Sg\}$ which is entirely contained in $\langle g \rangle$. Finally, g is a term of α by Proposition 4 as one of $s_1, \ldots, s_k$ equals 1.

4 The main result

The proof of the main theorem involves certain rearrangements of terms in zero-free sequences. The next lemma states a condition guaranteeing that such rearrangements are possible.

Lemma 6 *Let α be a zero-free sequence of length ℓ greater than $n/2$ in $\mathbb{Z}_n$. Suppose that, for some $k \in \{1, \ldots, \ell - 2\}$, the first $k + 1$ terms of α form a subsequence with sumset of size at least $2k+1$. Then the remaining terms of α can be rearranged so that the sequence obtained ends in a 1-term.*

PROOF. Regardless of how the last $\ell - k - 1$ terms of α are permuted, at least one of them will be a 1-term for the permuted sequence. If not, by Proposition 1 each term after the first $k + 1$ increases the sumset size by at least 2. Hence the total sumset size is at least $(2k+1)+2(\ell-k-1) = 2\ell-1 \geq n$ which is impossible for a zero-free sequence.

Fix the initial $k+1$ terms of α. Choose a rearrangement of the last $\ell-k-1$ terms such that the first 1-term among them occurs as late as possible. Let this term be c, and let α' be the resulting rearrangement of α. We are done if c is the last term of α'. If not, interchange c with any term d following it in α' to obtain a new rearrangement α''. The same sequence β precedes c and d in α' and α'', respectively, and β contains no 1-terms after the initial $k+1$ terms. On the other hand, by the extremal choice of α', a 1-term must occur among the last $\ell-k-1$ terms of α'' at the position of d in the latest. Therefore d is a 1-term for α''. Thus if either of c and d is appended to β, the sequence obtained ends in a 1-term. Now Proposition 2 c) implies $c=d$. Hence the terms after c in α' are all equal to c, so they are all 1-terms for α' by Proposition 2 a). In particular, α' ends in a 1-term. $\square$

Theorem 7 *Each zero-free sequence of length greater than $n/2$ in the cyclic group $\mathbb{Z}_n$ is behaving with respect to one of its terms.*

PROOF. First we prove the theorem for maximal sequences. Let α be a maximal zero-free sequence of length $\ell > n/2$ in $\mathbb{Z}_n$.

For each term a of α there exist a-behaving subsequences of α, for instance the one-term subsequence (a). We assign to a one such a-behaving subsequence $\alpha_a = (s_1a, \ldots, s_ka)$ of maximum length k. Here $(s_1, \ldots, s_k)$ is a behaving positive integer sequence such that $S = s_1 + \cdots + s_k$ is less than the order $\mathrm{ord}(a)$ of a in $\mathbb{Z}_n$. In particular $1 \le s_i < \mathrm{ord}(a)$, $i = 1, \ldots, k$. The sumset of $(s_1, \ldots, s_k)$ is $\{1, 2, \ldots, S\}$, and the sumset of α_a is $\{a, 2a, \ldots, Sa\}$, a progression contained in the cyclic subgroup $\langle a\rangle$ generated by a. Observe that all occurrences of a in α are terms of α_a.

We show that there is a term g whose associated g-behaving subsequence α_g is the entire α. To this end, choose an arbitrary term a of α and suppose that $\alpha_a \ne \alpha$. The notation for α_a from the previous paragraph is assumed. Let us rearrange α as follows. Write the terms of α_a first and then any term b of α which is not in α_a. The subsequence $\alpha_a \cup \{b\} = (s_1a, \ldots, s_ka, b)$ obtained so far has sumset $P_1 \cup P_2$ where $P_1 = \{a, 2a, \ldots, Sa\}$ and $P_2 = \{b, b+a, \ldots, b+Sa\}$.

It is not hard to check that $P_1 \cap P_2 = \emptyset$. This is clear if $b \notin \langle a\rangle$ as P_1 and P_2 are in different cosets of $\langle a\rangle$. Let $b \in \langle a\rangle$, so $b = sa$ with $1 \le s < \mathrm{ord}(a)$. Then $P_2 = \{sa, (s+1)a, \ldots, (s+S)a\}$ and it suffices to prove the inequalities $S+1 < s$ and $s+S < \mathrm{ord}(a)$.

First, $s+S \ge \mathrm{ord}(a)$ implies that $\mathrm{ord}(a)$ occurs among the consecutive integers $s, s+1, \ldots, s+S$. Hence P_2 contains the zero element of $\mathbb{Z}_n$ which is false. Next, suppose that $s \le S+1$. Then the integer sequence $(s_1, \ldots, s_k, s)$ has sum $s+S$ and sumset $\{1, \ldots, S, \ldots, s+S\}$, so it is behaving. We also have $s+S < \mathrm{ord}(a)$, as just shown. But then $\alpha_a \cup \{b\} = (s_1a, \ldots, s_ka, sa)$ is an a-behaving subsequence of α longer than α_a, contradicting the maximum choice of α_a. Therefore P_1 and P_2 are disjoint also in the case $b \in \langle a\rangle$.

Now, $P_1 \cap P_2 = \emptyset$ and $|P_1| = S \geq k$, $|P_2| = S + 1 \geq k + 1$ imply that $|P_1 \cup P_2| \geq 2k + 1$. It also follows that there are terms of α out of $\alpha_a \cup \{b\}$. Otherwise $k + 1 = \ell$ and because $n - 1 \geq |P_1 \cup P_2| \geq 2k + 1$ ($\alpha_a \cup \{b\}$ is zero-free, hence its sumset has size at most $n - 1$), we obtain $n \geq 2\ell$ which is not the case. Therefore, by Lemma 6, the terms of α not occurring in $\alpha_a \cup \{b\}$ can be permuted to obtain a rearrangement α' which ends in a 1-term c.

Recall now that α is maximal, and hence so is its rearrangement α'. Let Σ be the sumset of the sequence obtained from α' by deleting its last term c. Since c is a 1-term for α', Σ is missing exactly one nonzero element of $\mathbb{Z}_n$. By Proposition 1, the missing element is the sum $A \neq 0$ of all terms of α. On the other hand, Σ must be missing the element $-c$ of $\mathbb{Z}_n$ ($-c \neq 0$), or else appending c to obtain α' would produce a zero sum. Because the missing element is unique, we obtain $A = -c$, i. e. $c = -A$.

We reach the following conclusion. If $\alpha_a \neq \alpha$ for at least one term a of α then the group element $-A$ is a term of α. Moreover, if a is any term such that $\alpha_a \neq \alpha$, the subsequence α_a does not contain at least one occurrence of $-A$.

Apply this conclusion to an arbitrary term g of α. The statement is proven if $\alpha_g = \alpha$. If not then $h = -A$ is a term of α. Consider its associated maximal h-behaving subsequence α_h. Since α_h contains all occurrences of $-A = h$, it follows that $\alpha_h = \alpha$. This completes the proof in the case where α is maximal.

Suppose now that α is not maximal. By Proposition 3, it can be extended to a maximal zero-free sequence β in $\mathbb{Z}_n$, of length $m > \ell > n/2$. (Clearly $m < n$.) By the above, there is a term a of β such that β is a-behaving. This is to say, $\beta = (s_1 a, \ldots, s_m a)$ for some behaving positive integer sequence $(s_1, \ldots, s_m)$ with sum less than $\operatorname{ord}(a)$. Deleting the additionally added terms from β, we infer that $\alpha = (s_{i_1} a, \ldots, s_{i_\ell} a)$ for some positive integer sequence $(s_{i_1}, \ldots, s_{i_\ell})$ of length ℓ and sum less than $\operatorname{ord}(a)$. Now, since $\ell > n/2 \geq \operatorname{ord}(a)/2$, one can apply Proposition 5 with $k = \operatorname{ord}(a)$, which shows that $(s_{i_1}, \ldots, s_{i_\ell})$ is behaving. Hence $\alpha = (s_{i_1} a, \ldots, s_{i_\ell} a)$ is a-behaving. Also, a is a term of α: as already explained, one of the integers $s_{i_1}, \ldots, s_{i_\ell}$ equals 1 by Proposition 4. The proof is complete. $\square$

By Theorem 7, each zero-free sequence of length $\ell > n/2$ in $\mathbb{Z}_n$ has the form $\alpha = (s_1 a, \ldots, s_\ell a)$, where a is one of its terms and $(s_1, \ldots, s_\ell)$ is a positive integer sequence with sum less than $\operatorname{ord}(a)$. In particular $1 \leq s_i < \operatorname{ord}(a)$ for $i = 1, \ldots, \ell$. It is immediate that $\operatorname{ord}(a) = n$. Otherwise the subgroup $\langle a \rangle$, of order at most $n/2$, would contain a zero-free sequence of length $\ell > n/2$ which is impossible. Hence there is an integer g coprime to n such that $(s_1, \ldots, s_\ell)$ is the sequence of the least positive representatives for the equivalent sequence $g\alpha$. This is our main result.

Theorem 8 *Each zero-free sequence of length greater than $n/2$ in the cyclic group $\mathbb{Z}_n$ is equivalent to a sequence whose sum of the least positive representatives is less than n.*

Such a conclusion does not hold in general for shorter sequences in $\mathbb{Z}_n$. Zero-free sequences with lengths at most $n/2$ and failing Theorem 8 are not hard to find. Consider for example the following sequences in $\mathbb{Z}_n$:

$$\alpha = 2^{n/2-1}3 \quad \text{for even } n \geq 6 \qquad \text{and} \qquad \beta = 2^{(n-5)/2}3^2 \quad \text{for odd } n \geq 9.$$

Here and further on, multiplicities of sequence terms are indicated by using exponents; for instance $1^3 2^2 3$ denotes the sequence $(1, 1, 1, 2, 2, 3)$. Both α and β are zero-free, of lengths $n/2$ and $(n-1)/2$, respectively. One can check directly that for each g coprime to n the sequences $g\alpha$ and $g\beta$ have sums of their least positive representatives greater than n.

5 The index of a long minimal zero sequence

Chapman, Freeze and Smith defined the *index* of a sequence in [3]. Given a sequence α in $\mathbb{Z}_n$, its index $Index(\alpha)$ is defined as the minimum of $L(g\alpha)$ over all integers g coprime to n. (Recall that $L(\omega)$ denotes the sum of the least positive representatives of the sequence ω.) In terms of the index, Theorem 8 can be stated as follows.

Theorem 9 *Each zero-free sequence of length greater than $n/2$ in $\mathbb{Z}_n$ has index less than n.*

The index of each nonempty zero sequence in $\mathbb{Z}_n$ is a positive multiple of n. A zero sequence in $\mathbb{Z}_n$ is *minimal* if each of its nonempty proper subsequences is zero-free. The question about the minimal zero sequences with index exactly n was studied from different points of view.

For instance, let $\ell(\mathbb{Z}_n)$ be the minimum integer such that every minimal zero sequence α in $\mathbb{Z}_n$ of length at least $\ell(\mathbb{Z}_n)$ satisfies $Index(\alpha) = n$. Gao [6] proved the estimates $\lfloor (n+1)/2 \rfloor + 1 \leq \ell(\mathbb{Z}_n) \leq n - \lfloor (n+1)/3 \rfloor + 1$ for $n \geq 8$ ($\lfloor x \rfloor$ denotes the greatest integer not exceeding x). Based on Theorem 8, here we determine $\ell(\mathbb{Z}_n)$ for all n.

The proof comes down to the observation that each minimal zero sequence of length greater than $n/2+1$ in $\mathbb{Z}_n$ has index n. Indeed, remove one term a from such a sequence α; this yields a zero-free sequence α' of length greater than $n/2$. By Theorem 9, $Index(\alpha') < n$. Since $\overline{ga} \leq n$ for any integer g, it follows that $Index(\alpha) \leq Index(\alpha') + n < 2n$. So $Index(\alpha) = n$, and we obtain $\ell(\mathbb{Z}_n) \leq \lfloor n/2 \rfloor + 2$ for all n. Now consider the following sequences in $\mathbb{Z}_n$:

$$\alpha = 2^{n/2-1}3(-1) \text{ for even } n \geq 6 \quad \text{and} \quad \beta = 2^{(n-5)/2}3^2(-1) \text{ for odd } n \geq 9.$$

These modifications of the examples at the end of the previous section show that the upper bound $\ell(\mathbb{Z}_n) \leq \lfloor n/2 \rfloor + 2$ is tight for even $n \geq 6$ and odd $n \geq 9$. Indeed, α and β are minimal zero sequences, of respective lengths $n/2+1$ and $(n+1)/2$. In both cases the length equals $\lfloor n/2 \rfloor + 1$. By the conclusion from the last paragraph of Section 4, each of α and β has index greater than n. (In fact $Index(\alpha) = Index(\beta) = 2n$.)

For the values of n not covered by these examples, that is $n = 2, 3, 4, 5, 7$, it is proven in [3] that $\ell(\mathbb{Z}_n) = 1$. It remains to summarize the conclusions.

Proposition 10 *The values of $\ell(\mathbb{Z}_n)$ for all $n > 1$ are: If $n \notin \{2, 3, 4, 5, 7\}$ then $\ell(\mathbb{Z}_n) = \lfloor n/2 \rfloor + 2$; if $n \in \{2, 3, 4, 5, 7\}$ then $\ell(\mathbb{Z}_n) = 1$.*

6 The maximum multiplicity of a term

An extensively used result of Bovey, Erdős and Niven [2] states that each zero-free sequence of length $\ell > n/2$ in $\mathbb{Z}_n$ contains a term of multiplicity at least $2\ell - n + 1$. The authors remark that this estimate is best possible whenever $(2n-2)/3 \le \ell < n$. An improvement for the more interesting range $n/2 < \ell \le (2n-2)/3$ is due to Gao and Geroldinger [7] who showed that $2\ell - n + 1$ can be replaced by $\max(2\ell - n + 1, \ell/2 - (n-4)/12)$ (for $\ell \ge (n+3)/2$). Here we obtain a sharp lower bound for each length ℓ greater than $n/2$.

Let M be the maximum multiplicity of a term in a zero-free sequence α with length $\ell > n/2$ in $\mathbb{Z}_n$. Clearly M has the same value for all sequences equivalent to α, and also for the respective sequences of least positive representatives. Therefore, by Theorem 8, one may assume that α is a positive integer sequence of length $\ell > n/2$ and sum $S \le n-1$. Let α contain u ones and v twos. Then

$$n-1 \ge S \ge u+2(\ell-u) = 2\ell-u, \; n-1 \ge S \ge u+2v+3(\ell-u-v) = 3\ell-2u-v.$$

These yield $u \ge 2\ell - n + 1$ and $2u + v \ge 3\ell - n + 1$, respectively. Since $M \ge \max(u, v)$, it follows that $M \ge \max(2\ell - n + 1, \ell - \lfloor (n-1)/3 \rfloor)$. Now, $2\ell - n + 1 \ge \ell - \lfloor (n-1)/3 \rfloor$ if and only if $\ell \ge (2n-2)/3$, so two cases arise.

For $(2n-2)/3 \le \ell < n$, the lower bound $M \ge 2\ell - n + 1$ is best possible, as already remarked in [2]. Indeed, $\alpha = 1^{2\ell-n+1} 2^{n-\ell-1}$ is a well-defined positive integer sequence whenever $n/2 < \ell < n$ (note that the last inequality implies $n > 2$). It has length ℓ and sum $n-1$. If in addition $(2n-2)/3 \le \ell < n$ then $2\ell - n + 1$ is the maximum multiplicity of a term in α, so $M = 2\ell - n + 1$.

If $n/2 < \ell \le (2n-2)/3$, the lower bound $M \ge \ell - \lfloor (n-1)/3 \rfloor$ is best possible. To show that the equality can be attained, consider the sequence

$$\alpha = 1^{\ell - \lfloor (n-1)/3 \rfloor} 2^{\ell - \lfloor (n-1)/3 \rfloor} 3^{2\lfloor (n-1)/3 \rfloor - \ell}.$$

It is well defined unless n is divisible by 3 and $\ell = 2n/3 - 1$; this case will be considered separately. The multiplicities of 1, 2 and 3 are nonnegative integers for all other values of n and ℓ satisfying $n/2 < \ell \le (2n-2)/3$ (which also implies $n > 3$). So α is a positive integer sequence with length ℓ, sum $3\lfloor (n-1)/3 \rfloor \le n - 1$ and two terms of maximum multiplicity which equals $\ell - \lfloor (n-1)/3 \rfloor$. In the exceptional case mentioned above, the example $\alpha = 1^{n/3} 2^{n/3-1}$ shows that $M = \ell - \lfloor (n-1)/3 \rfloor$ is attainable, too.

We proved the following tight piecewise linear lower bound.

Proposition 11 *Let n and ℓ be integers satisfying $n/2 < \ell < n$. Each zero-free sequence of length ℓ in $\mathbb{Z}_n$ has a term with multiplicity:*

a) at least $2\ell - n + 1$ *if* $(2n{-}2)/3 \le \ell < n$*;*
b) at least $\ell - \lfloor (n{-}1)/3 \rfloor$ *if* $n/2 < \ell \le (2n{-}2)/3$.
These estimates are best possible.

Essentially speaking, the arguments above yield an explicit description of the zero-free sequences in $\mathbb{Z}_n$ with a given length $\ell > n/2$. This description is included in Section 9. Here we only note that the equality $M = \max(u, v)$ holds for each positive integer sequence α of length greater than $n/2$ and sum at most $n{-}1$. Indeed, fix $2\ell - n + 1$ ones in α (this many ones are available in view of $u \ge 2\ell - n + 1$). The remaining part α' has length $n - 1 - \ell$ and sum $\le 2(n - 1 - \ell)$, so the average of its terms is at most 2. It readily follows that α' contains at least as many ones as terms greater than 2.

7 The maximum multiplicity of a generator

Given a zero-free sequence in $\mathbb{Z}_n$, what can be said about the number of generators it contains? As usual, here a *generator* means an element of $\mathbb{Z}_n$ with order n. This question attracted considerable attention and effort, for sequences of length greater than $n/2$. Even the existence of one generator in such a sequence (which follows directly from Theorem 7) does not seem immediate. It was proven by Gao and Geroldinger [7]. Improving on their result, Geroldinger and Hamidoune [8] obtained the following theorem. A zero-free sequence α of length at least $(n{+}1)/2$ in $\mathbb{Z}_n$ ($n \ge 3$) contains a generator with multiplicity 3 if n is even, and with multiplicity $\lceil (n{+}5)/6 \rceil$ if n is odd ($\lceil x \rceil$ denotes the least integer greater than or equal to x). These bounds are sharp if α ranges over the zero-free sequences in $\mathbb{Z}_n$ of *all* lengths $\ell \ge (n{+}1)/2$.

On the other hand, the above estimates do not reflect the length of α. One can be more specific by finding best possible bounds for each length ℓ in the range $(n/2, n)$.

Denote by m the maximum multiplicity of a generator in a zero-free sequence α with length $\ell > n/2$ in $\mathbb{Z}_n$. By Theorem 8, we may assume again that α is a positive integer sequence of length $\ell > n/2$ and sum at most $n{-}1$; the point of interest now is the maximum multiplicity m of a term coprime to n. Let α contain u ones and v twos, as in Section 6. It was shown there that $u \ge 2\ell - n + 1$, and because 1 is coprime to n, we have $m \ge 2\ell - n + 1$.

If n is even, the sequence $1^{2\ell - n+1} 2^{n-\ell-1}$ shows that this bound is sharp.

If n is odd then 2 is coprime to n, so $m \ge \max(u, v)$. But if M is the maximum multiplicity of a term in α then $m \le M$, and also $M = \max(u, v)$ by the remark after Proposition 11. Hence $M = m$, so the answer in the case of an odd n coincides with the one from the previous section.

The conclusions are stated in the next proposition.

Proposition 12 *Let* n *and* ℓ *be integers satisfying* $n/2 < \ell < n$*, and let* α *be a zero-free sequence of length* ℓ *in* $\mathbb{Z}_n$*.*

a) For n *even,* α *contains a generator of multiplicity at least* $2\ell - n + 1$*. This*

estimate is best possible.

b) *For n odd, α contains a generator of multiplicity at least $2\ell - n + 1$ if $(2n-2)/3 \le \ell < n$, and at least $\ell - \lfloor (n-1)/3 \rfloor$ if $n/2 < \ell \le (2n-2)/3$. These estimates are best possible.*

The theorem of Geroldinger and Hamidoune [8] can be regarded as an extremal case of Proposition 12, obtained by setting $\ell = n/2 + 1$ if n is even, and $\ell = (n+1)/2$ if n is odd.

8 A function related to zero-free sequences

For positive integers n and k, where $n \ge k$, let $h(n,k) \ge k$ be the least integer such that each sequence in $\mathbb{Z}_n$ with at least k distinct terms and length $h(n,k)$ contains a nonempty zero sum. The function $h(n,k)$ is a natural analogue of a function introduced by Bialostocki and Lotspeich [1] in relation to the renowned theorem of Erdős, Ginzburg and Ziv [5].

It is trivial to notice that $h(n,k) = k$ whenever k is greater than or equal to the *Olson's constant* of the group $\mathbb{Z}_n$. Olson's constant $Ol(G)$ of an abelian group G is the least positive integer t such that every subset of G with cardinality t contains a nonempty subset whose sum is zero. Erdős [4] conjectured that $Ol(G) \le \sqrt{2|G|}$ for each abelian group G; here $|G|$ is the order of G. The best known upper bound for $Ol(G)$ is due to Hamidoune and Zémor [9] who proved that $Ol(G) \le \left\lceil \sqrt{2|G|} + \gamma(|G|) \right\rceil$, where $\gamma(n) = O\left(n^{1/3} \log n\right)$. On the other hand, the set $\{1, 2, \ldots, k\}$ where k is the greatest integer such that $1 + 2 + \cdots + k < n$, yields the obvious lower bound $Ol(\mathbb{Z}_n) \ge \left\lfloor \left(\sqrt{8n-7} - 1\right)/2 \right\rfloor + 1$.

As for values of k less than $Ol(\mathbb{Z}_n)$, by using Theorem 8 one can determine $h(n,k)$ for all $k \le \left(\sqrt{4n-3} + 1\right)/2$.

Proposition 13 *Let $n \ge k$ be positive integers such that $k \le (\sqrt{4n-3}+1)/2$. Then*

$$h(n,k) = n - \frac{1}{2}(k^2 - k).$$

PROOF. The claim is true for $k = 1$, so let $k > 1$. Denote $\ell = n - (k^2 - k)/2$ and notice that $2 \le k \le \left(\sqrt{4n-3} + 1\right)/2$ is equivalent to $n/2 < \ell < n$. We show that each zero-free sequence α of length ℓ in $\mathbb{Z}_n$ contains fewer than k distinct terms; then $h(n,k) \le n - (k^2 - k)/2$ by the definition of $h(n,k)$.

By Theorem 8 one may regard α as a positive integer sequence of length ℓ and sum $S \le n-1$. An easy computation shows that α has at least $2\ell - S$ ones. So $\alpha = 1^{2\ell - S}\beta$, where β is a sequence of length $S - \ell$ and sum $2(S - \ell)$. Let there be m distinct terms in $1^{2\ell-S}\beta$; then β has $m - 1$ distinct terms greater than 1. Because $k > 1$, we may assume $m > 1$. Choose one occurrence for each of the $m-1$ distinct terms in β and replace these occurrences by $2, 3, \ldots, m$. Next, replace each remaining term by 1. The sum of β does not increase, so

$2(S-\ell) \geq (2+3+\cdots+m)+(S-\ell-m+1)$. Combined with $S \leq n-1$, this leads to $m^2-m-2(n-\ell-1) \leq 0$. Hence

$$m \leq \frac{1}{2}\left(\sqrt{8(n-\ell)-7}+1\right) = \frac{1}{2}\left(\sqrt{4(k^2-k)-7}+1\right) < k.$$

Therefore $2 \leq k \leq \left(\sqrt{4n-3}+1\right)/2$ implies $h(n,k) \leq n-(k^2-k)/2$.

Now consider the sequence $\alpha = 1^{\ell-k+1}23\dots k$, where $\ell = n-(k^2-k)/2-1$. Whenever $2 \leq k \leq \left(\sqrt{4n-3}+1\right)/2$ and $(n,k) \neq (3,2)$, there are k distinct terms in α because these conditions imply $\ell-k+1 \geq 1$. Also α has length $\ell \geq k$ and is zero-free since the sum of its least positive representatives is $n-1$. It follows that $h(n,k) \geq n-(k^2-k)/2$. The same lower bound holds for $n=3$, $k=2$ by the definition of $h(n,k)$. Hence $h(n,k) \geq n-(k^2-k)/2$ for all n and k satisfying $2 \leq k \leq \left(\sqrt{4n-3}+1\right)/2$, which completes the proof. □

The example $\alpha = 1^{\ell-k+1}23\dots k$ in the last proof yields the lower bound $h(n,k) \geq n-(k^2-k)/2$ for $k \leq \left(\sqrt{8n-7}-1\right)/2$ which is a weaker constraint than $k \leq \left(\sqrt{4n-3}+1\right)/2$ if $n > 7$. So the following query is in order here.

Question 14 *Does the equality*

$$h(n,k) = n-\frac{1}{2}(k^2-k)$$

hold true whenever $k \leq \left(\sqrt{8n-7}-1\right)/2$*?*

9 Concluding remarks

Among other consequences, Theorem 8 yields various explicit descriptions of the zero-free sequences in $\mathbb{Z}_n$ with a given length $\ell > n/2$. We include one such description mentioned in Section 6, skipping over the easy justification.

Let n and ℓ be integers satisfying $n/2 < \ell < n$. An arbitrary zero-free sequence α of length ℓ in $\mathbb{Z}_n$ has one of the equivalent forms specified below.

1. If $(2n-2)/3 \leq \ell < n$ then $\alpha \cong 1^u\beta$, where $u \geq 2\ell-n+1$ and β is a sequence of length $\ell-u$ in $\mathbb{Z}_n$, without ones and satisfying $L(\beta) \leq n-1-u$.
2. If $n/2 < \ell \leq (2n-2)/3$ there are two possibilities:
   a) $\alpha \cong 1^u\beta$, where $u \geq \ell/2$ and β is a sequence of length $\ell-u$ in $\mathbb{Z}_n$, without ones and satisfying $L(\beta) \leq n-1-u$.
   b) $\alpha \cong 1^u2^v\beta$, where

$$u \leq \frac{\ell}{2}, \quad \min(u,v) \geq 2\ell-n+1, \quad \max(u,v) \geq \ell-\left\lfloor\frac{n-1}{3}\right\rfloor,$$

   and β is a sequence of length $\ell-u-v$ in $\mathbb{Z}_n$, without ones and twos and satisfying $L(\beta) \leq n-1-u-2v$.

A closer look at the description shows that the structure of the zero-free sequences with lengths ℓ satisfying $n/2 < \ell \leq (2n-2)/3$ is significantly more involved than the one for ℓ in the range $(2n-2)/3 \leq \ell < n$ considered in [6].

Yet another application of the main result concerns zero-sum problems of a different flavor. Let n and k be integers such that $n/2 < k < n$. By using Theorem 8, one can determine the structure of the sequences in $\mathbb{Z}_n$ with length $n-1+k$ that do not contain n-term zero subsequences. Such a characterization in turn has consequences related to variants of the Erdős–Ginzburg–Ziv theorem [5] and deserves separate treatment. Questions of this kind will be considered in a forthcoming article.

References

[1] A. Bialostocki, M. Lotspeich, Some developments of the Erdős–Ginzburg–Ziv theorem. I., in: Sets, Graphs and Numbers (Budapest, 1991), 97–117, Colloq. Math. Soc. János Bolyai 60, North-Holland, Amsterdam, 1992.

[2] J. D. Bovey, P. Erdős and I. Niven, Conditions for a zero sum modulo n, Canad. Math. Bull. 18 (1) (1975), 27–29.

[3] S. T. Chapman, M. Freeze and W. W. Smith, Minimal zero-sequences and the strong Davenport constant, Discrete Math. 203 (1–3) (1999), 271–277.

[4] P. Erdős, Problems and results on combinatorial number theory, in: A Survey of Combinatorial Theory, J. N. Srivastava et al. (eds.), North-Holland, Amsterdam, 1973, 117–138.

[5] P. Erdős, A. Ginzburg and A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel 10F (1961), 41–43.

[6] W. D. Gao, Zero sums in finite cyclic groups, Integers 0 (2000), A12, 7pp. (electronic).

[7] W. D. Gao, A. Geroldinger, On the structure of zerofree sequences, Combinatorica 18 (4) (1998), 519–527.

[8] A. Geroldinger, Y. O. Hamidoune, Zero-sumfree sequences in cyclic groups and some arithmetical application, J. Théor. Nombres Bordeaux 14 (1) (2002), 221–239.

[9] Y. O. Hamidoune, G. Zémor, On zero-free subset sums, Acta Arith. 78 (2) (1996), 143–152.

[10] W. W. Smith, M. Freeze, Sumsets of zerofree sequences, Arab. J. Sci. Eng. Sect. C Theme Issues 26 (1) (2001), 97–105.